(12) UK Patent Application (19) GB (11) 2 394 327 (13) A

(43) Date of A Publication 21.04.2004

(21) Application No: 0311729.8

(22) Date of Filing: 21.05.2003

(30) Priority Data:
(31) 0224228 (32) 17.10.2002 (33) GB
(31) 0307248 (32) 28.03.2003

(71) Applicant(s):
**Vodafone Group PLC**
**(Incorporated in the United Kingdom)**
**Vodafone House, The Connection,**
**NEWBURY, Berkshire, RG14 2FN,**
**United Kingdom**

(72) Inventor(s):
**David Jeal**
**George Stronach Mudie**

(74) Agent and/or Address for Service:
**Mathisen Macara & Co**
**The Coach House, 6-8 Swakeleys Road,**
**Ickenham, UXBRIDGE, Middlesex,**
**UB10 8BZ, United Kingdom**

(51) INT CL[7]:
**G06F 1/00**

(52) UK CL (Edition W ):
**G4A** AAP A23D

(56) Documents Cited:
**WO 2002/091316 A** **WO 2001/080525 A**
**WO 2000/070533 A** **WO 2000/002407 A**
**US 6226744 B**

(58) Field of Search:
INT CL[7] **G06F, G07F, H04L**
Other: **Online: WPI, EPODOC**

(54) Abstract Title: **A device for authenticating data communications over a network using a Smart or SIM card**

(57) A device or "dongle" (30) for controlling communications between a Subscriber Identity Module (or SIM) (12), such as of the type used in a GSM cellular telephone system, and a computer, such as a Windows-based PC (10). The SIM (12) can be authenticated by the telephone network, in the same way as for authenticating SIMs of telephone handset users in the network, and can in this way authenticate the user of the PC (10) or the PC (10) itself. Such authentication can, for example, permit use of the PC (10) for a time-limited session in relation to a particular application which is released to the PC (10) after the authentication is satisfactorily completed. The application may be released to the PC (10) by a third party after and in response to the satisfactory completion of the authentication process. A charge for the session can be debited to the user by the telecommunications network and then passed on to the third party. The dongle (30) provides additional security for the authentication data stored on the SIM by requiring a PIN to be entered and/or by only being responsive to requests received from the PC (10) which are encrypted using a key, which requests are generated by a special PC interface driver (38). The PIN may be stored only temporarily. The dongle (30) has an electrical connector (34), and means may be provided for selectively rendering the connector (34) available for coupling to the PC(10).

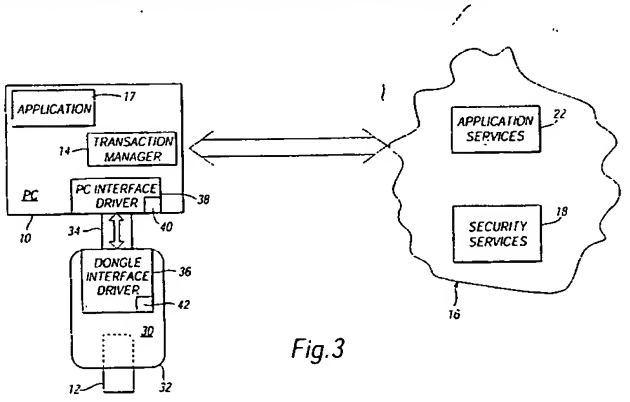


Fig.3



GB 2 394 327 A

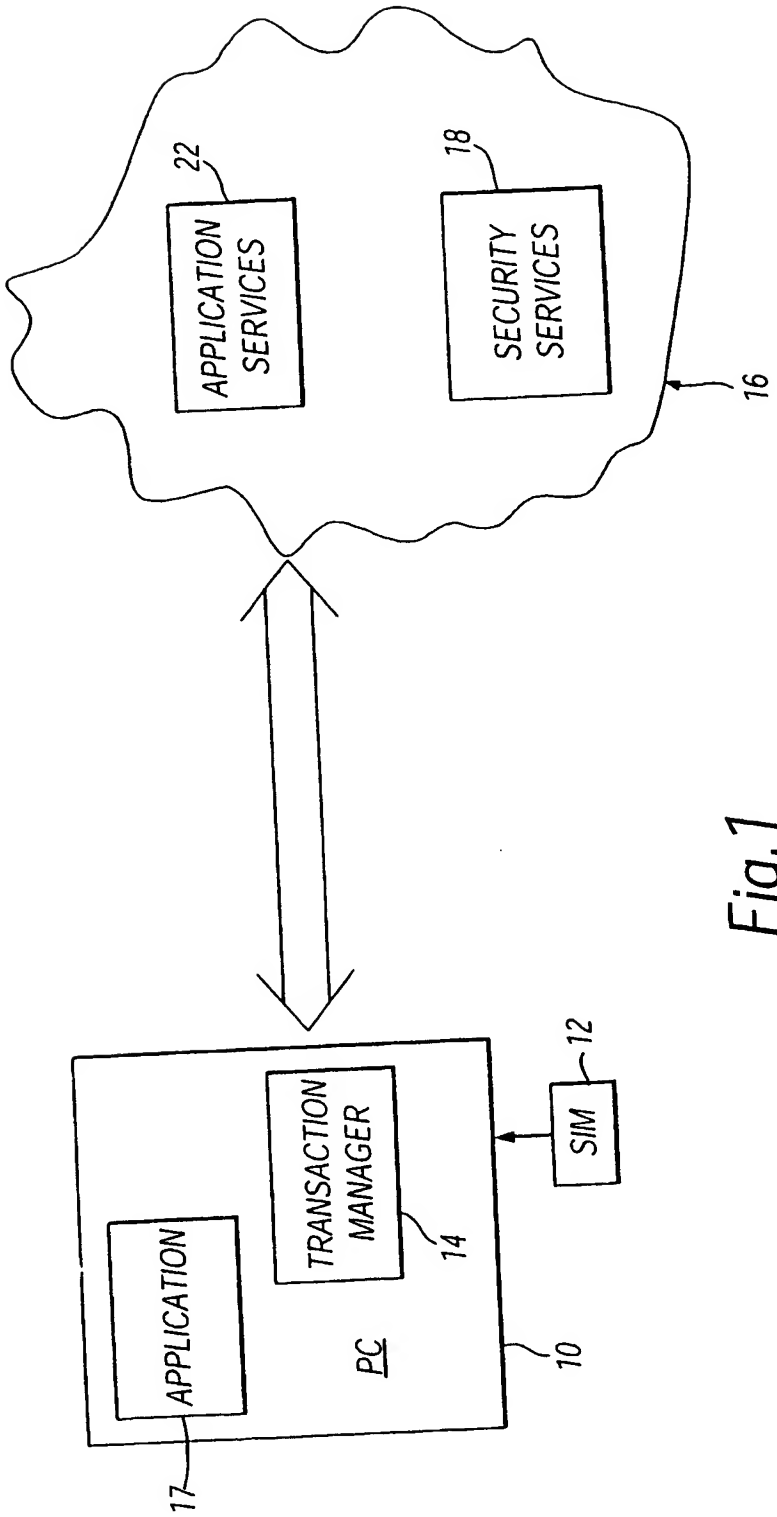
APPLICATION SERVICES
22
SECURITY SERVICES
18
16
TRANSACTION MANAGER
14
SIM
12
APPLICATION
17
PC
10

Fig.1

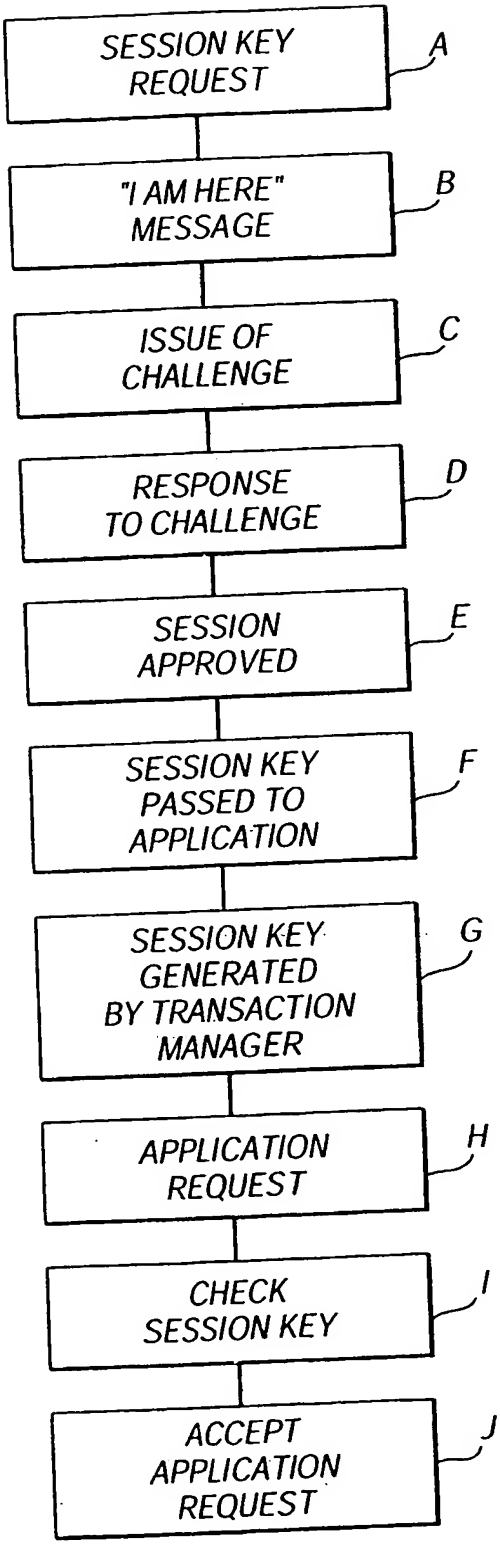
SESSION KEY REQUEST
A
"I AM HERE" MESSAGE
B
ISSUE OF CHALLENGE
C
RESPONSE TO CHALLENGE
D
SESSION APPROVED
E
SESSION KEY PASSED TO APPLICATION
F
SESSION KEY GENERATED BY TRANSACTION MANAGER
G
APPLICATION REQUEST
H
CHECK SESSION KEY
I
ACCEPT APPLICATION REQUEST
J

Fig.2

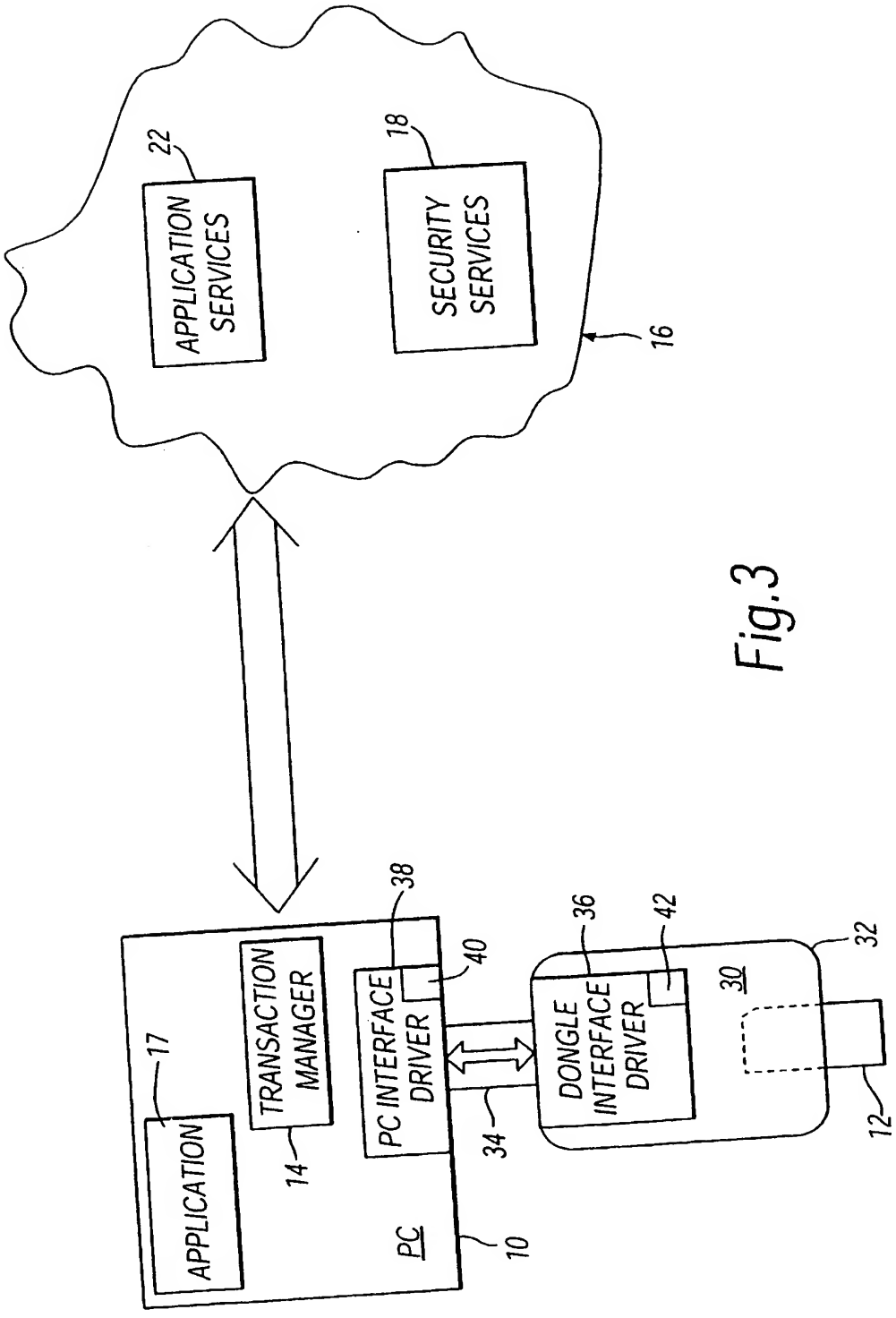
APPLICATION SERVICES
22
SECURITY SERVICES
18
16
APPLICATION
17
TRANSACTION MANAGER
14
PC INTERFACE DRIVER
38
40
PC
10
34
DONGLE INTERFACE DRIVER
36
42
30
32
12

Fig.3

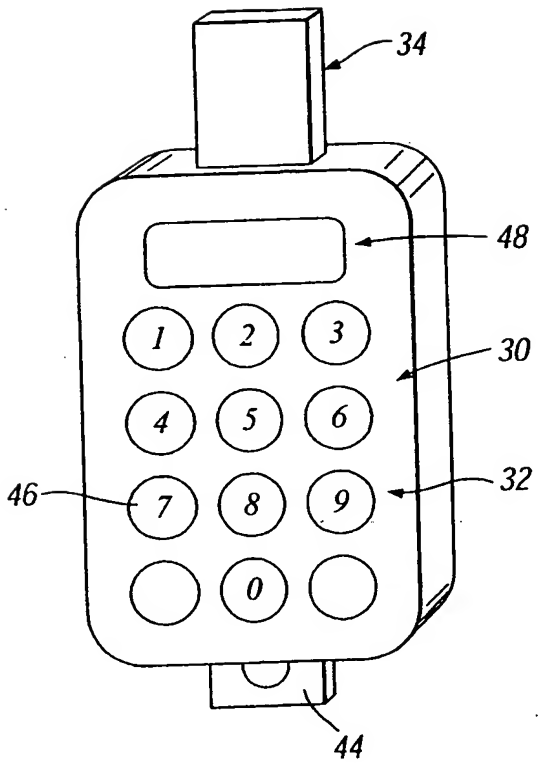


Fig.4

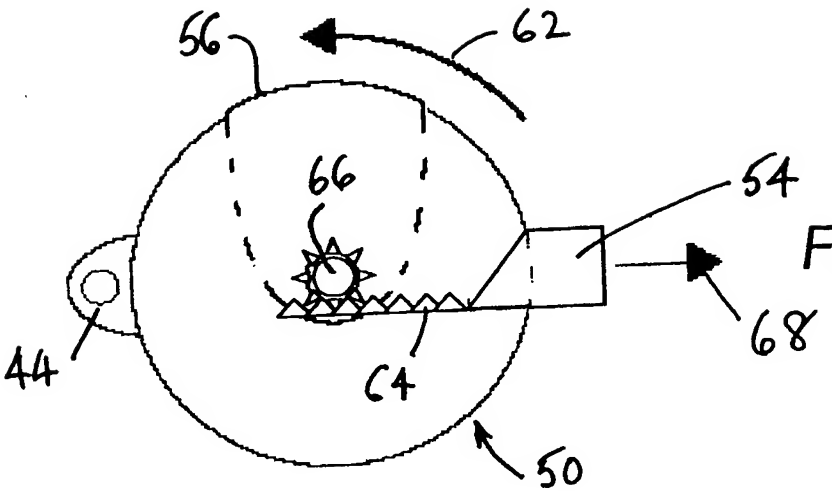


Fig. 5C

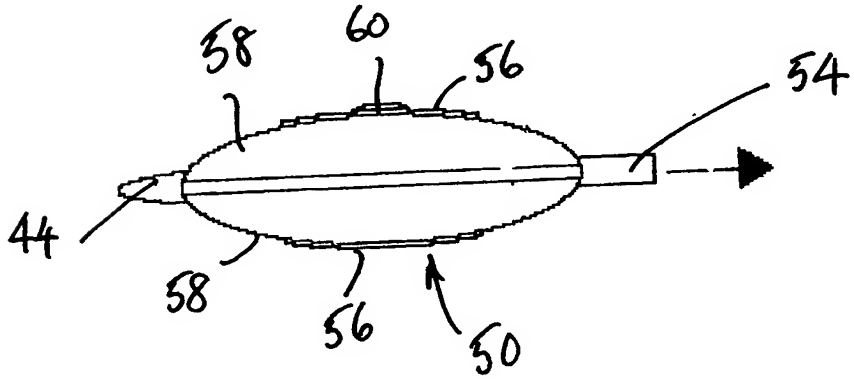


Fig. 5D

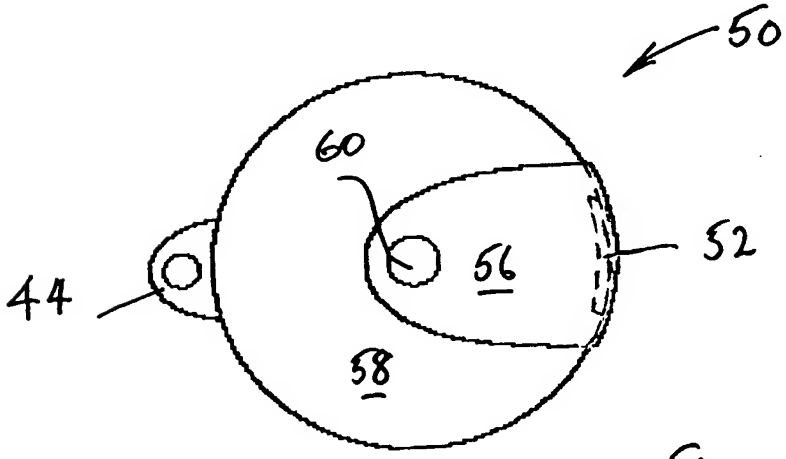


Fig. 5A

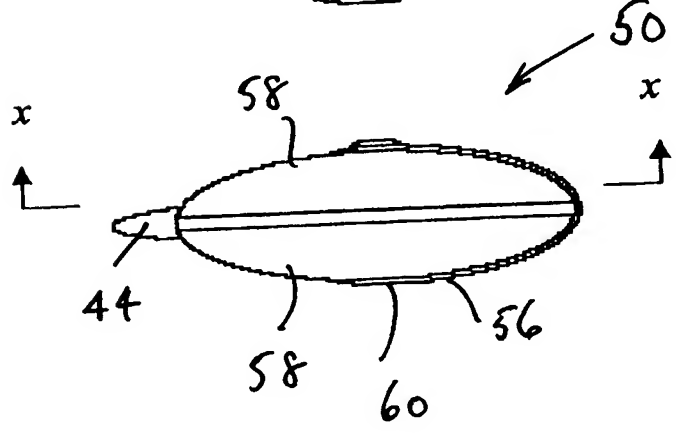


Fig. 5B

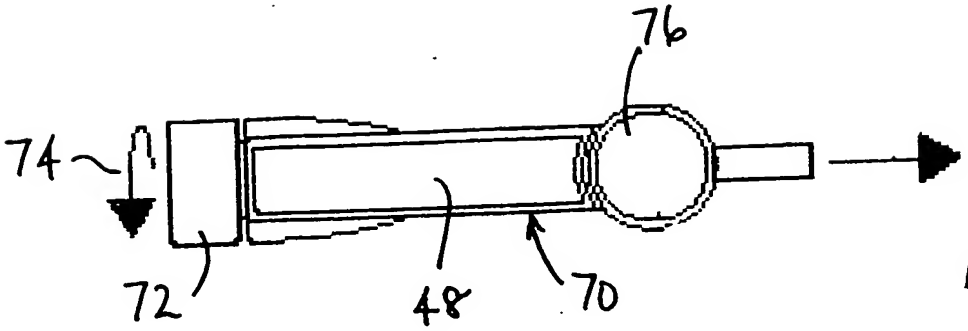


Fig. 6C

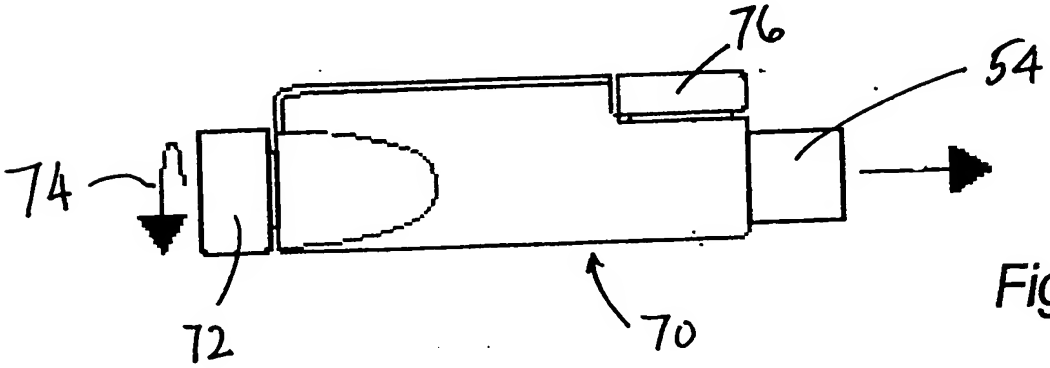


Fig. 6D

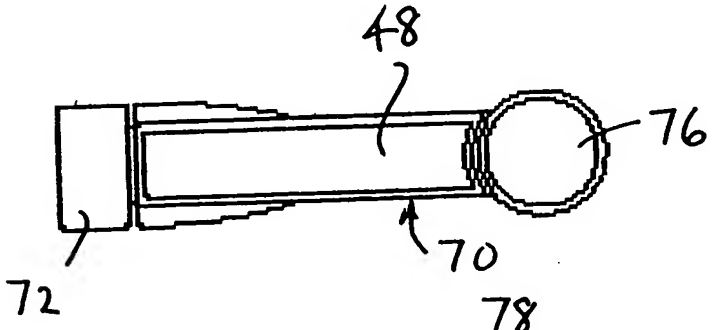


Fig. 6A

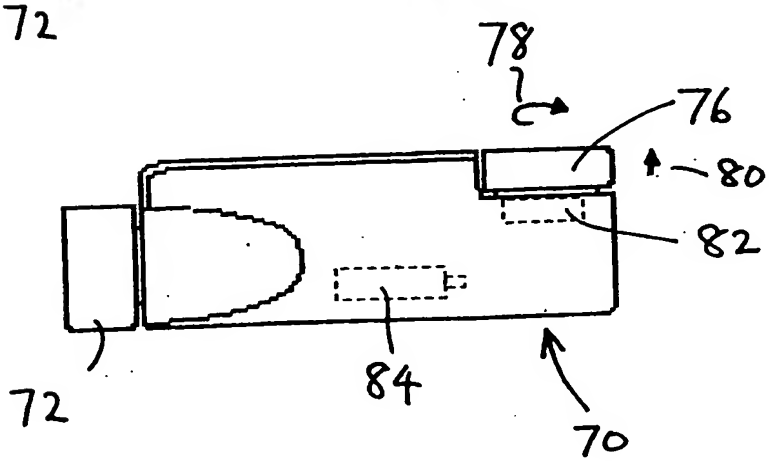


Fig. 6B

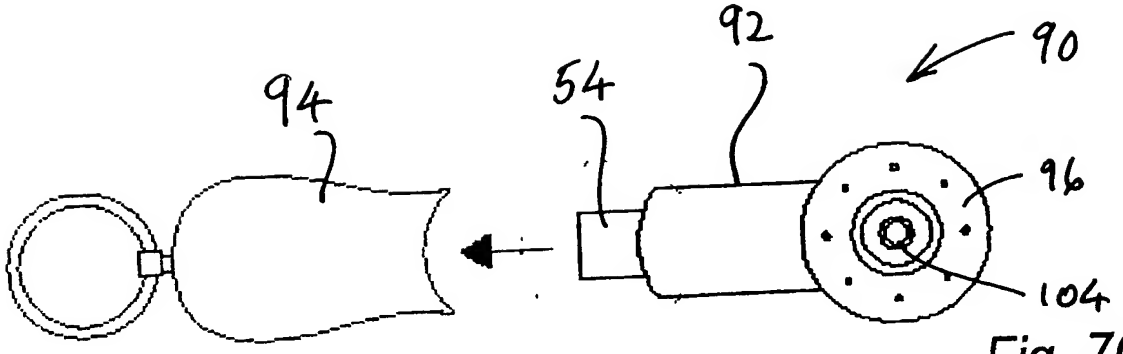


Fig. 7C

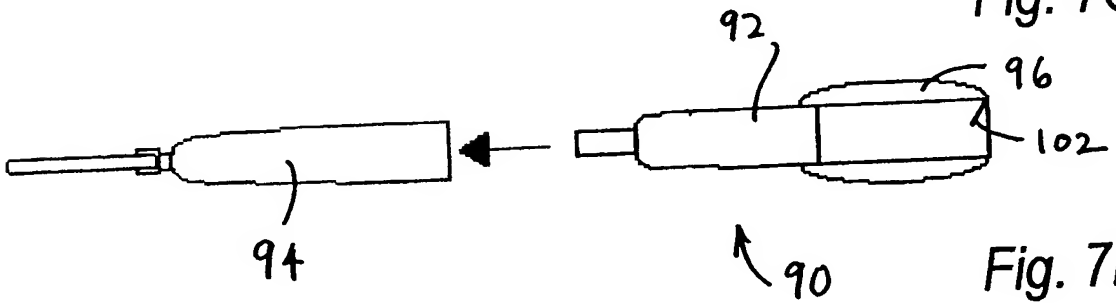


Fig. 7D

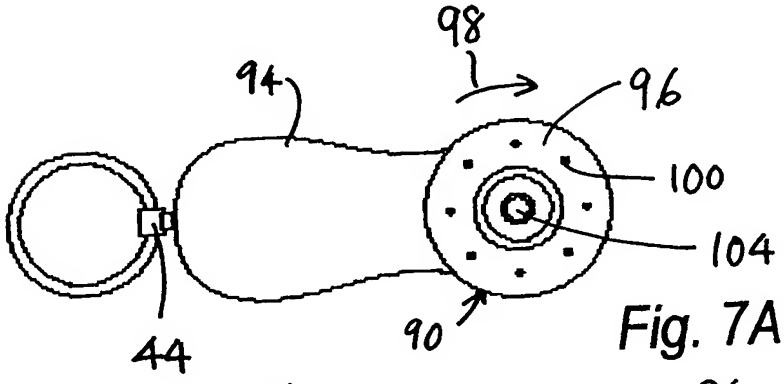


Fig. 7A

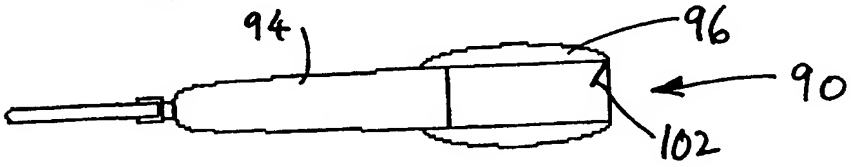


Fig. 7B

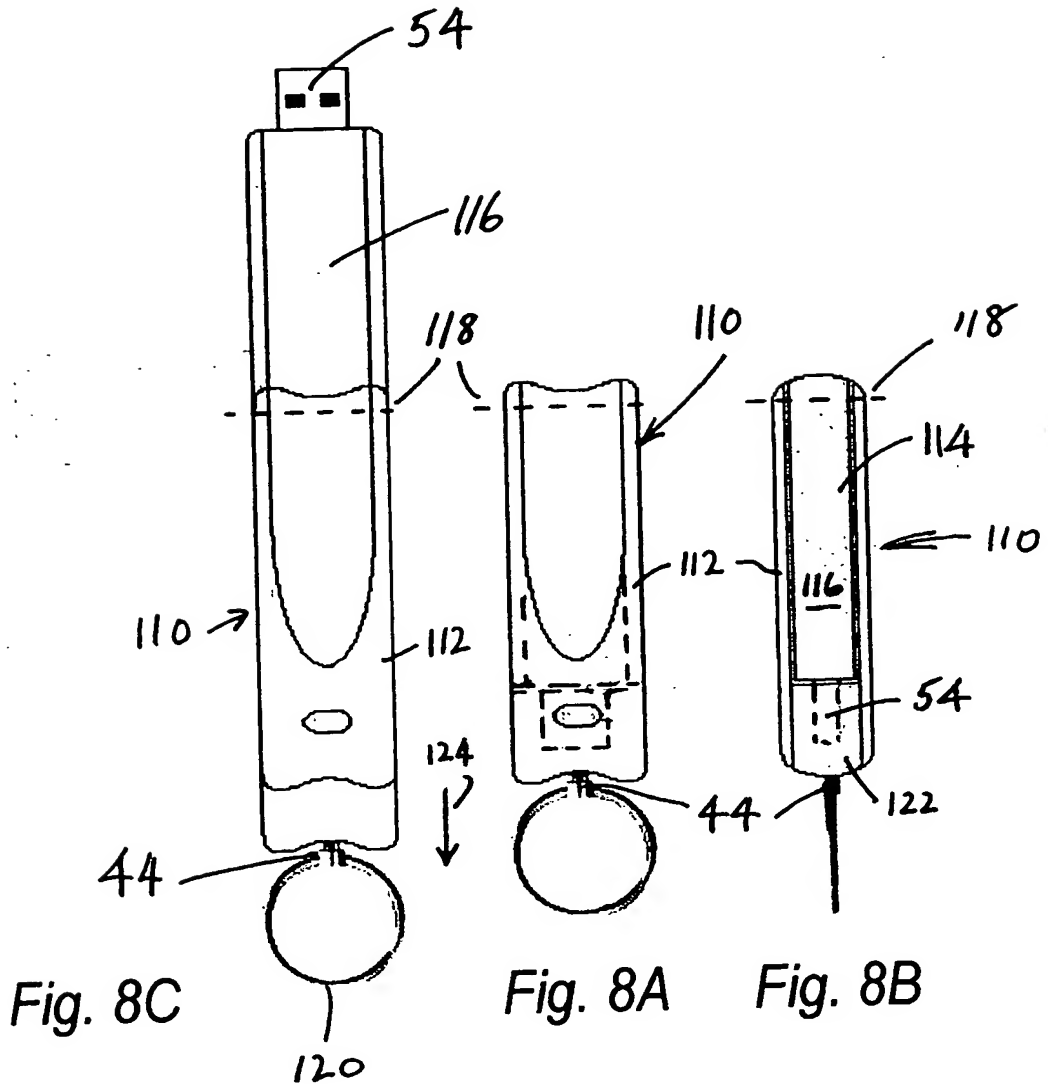


Fig. 8C Fig. 8A Fig. 8B

# DEVICE FOR FACILITATING AND AUTHENTICATING TRANSACTIONS

The invention relates to a device for the facilitation and authentication of transactions. In embodiments of the invention, to be described below in more detail by way of example only, transactions between data processing apparatus (such as a personal computer), or a user thereof, and a (possibly remote) third party are facilitated and authenticated by the device (or "dongle"), and such facilitation and authentication may also involve the facilitation and authentication of a payment to be made by or on behalf of the user to the third party.

According to the invention, there is provided a device for connection to a data processing apparatus, the device including first coupling means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus; second coupling means for operative coupling to the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information; security data entry means for obtaining security data independently of the data processing apparatus; and means for storing the security data temporarily.

According to the invention, there is also provided a device for connection to a data

processing apparatus, the device including first coupling means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus; second coupling means for operative coupling to the data processing apparatus; and configuration means for selectively rendering the second coupling means available for coupling to the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined configuration information.

Devices for connection to data processing apparatus (such as a personal computer) embodying the invention, will now be described, by way of example only, with reference to the accompanying diagrammatic drawings in which:

Figure 1 is a block diagram for explaining the operation of the method in relation to the data processing apparatus;

Figure 2 is a flow chart for use in the understanding of the block diagram of Figure 1;

Figure 3 is a block diagram corresponding to Figure 1 in which a "dongle" is used; and

Figure 4 is a perspective view of one configuration of a dongle;

Figure 5A shows a front view of a second configuration of a dongle;

Figure 5B shows a side view of the dongle of Figure 5A;

Figure 5C shows a cross-sectional view taken along line x-x of Figure 5B but with the dongle connector extended;

Figure 5D shows a side view corresponding to Figure 5B but with the dongle connector extended;

Figure 6A shows a front view of a third configuration of a dongle;

Figure 6B shows a side view of the dongle of Figure 6A;

Figure 6C shows a front view corresponding to Figure 6A but with the dongle connector extended;

Figure 6D shows a side view corresponding to Figure 6B but with the dongle connector extended;

Figure 7A shows a front view of a fourth configuration of a dongle;

Figure 7B shows a side view of the dongle of Figure 7A;

Figure 7C shows a front view corresponding to Figure 7A but with the dongle connector extended;

Figure 7D shows a side view corresponding to Figure 7B but with the dongle connector extended;

Figure 8A shows a front view of a fifth configuration of a dongle;

Figure 8B shows a side view of the dongle of Figure 8A; and

Figure 8C shows how the electrical connector emerges from the casing of the dongle.

In the figures like elements are generally designated with the same reference numbers.

There exist many instances when a transaction involving the use of data processing apparatus requires authentication. For example, the data processing apparatus may be required to carry out a transaction, such as the exchange of information, with a third party, such as a remote third party with which the communication must be made over a telecommunications link (including via the Internet). The third party may require that the

data processing apparatus, or the user thereof for the time being, is authenticated to the satisfaction of the third party before the transaction takes place.

As stated, the transaction may merely involve the exchange of information. For example, the user of the data processing apparatus may simply need to be authenticated in order to download information from the third party. Such information may be information kept by the third party on behalf of the user of the data processing apparatus (for example, information relating to the user's bank account). Instead, the information might be information held on other data processing apparatus, such as a data network belonging to an organisation or commercial entity with which the user is connected or by whom the user is employed, thus facilitating access to that network by the user when the user is travelling. Another possible transaction may involve the downloading by the data processing apparatus of software from the remote location.

In addition, the transaction may require a payment to be made by the user in order to enable the transaction to take place, such as a payment to the third party in return for the information provided. Clearly, when such a payment is involved, it is important that the user is authenticated to the satisfaction of the third party and that the payment is made in a safe, simple and secure manner.

Although the foregoing discussion has referred to a "user" of the data processing apparatus, some at least of the transactions described above may not in fact involve any

human user: the data processing apparatus may be required to operate automatically (for example, intermittently operating in an information-gathering or monitoring role, and reporting the results to a third party). In such cases, it may also be necessary for the data processing apparatus to authenticate itself to the satisfaction of the third party.

As described in our co-pending patent application No. GB 0224228.7, the data processing apparatus is provided with, or associated with, means (authentication storage means) for storing predetermined authentication information for authenticating that apparatus or a particular user thereof. In one embodiment, the means for storing the predetermined information is removable and can thus be taken by the user and inserted into any data processing apparatus (or computer) which is adapted to receive it, so as to enable that user to be authenticated in respect to a transaction to be carried out by that user with that computer. Advantageously, in such a case the means for storing the predetermined information is in the form of a smart card.

In a more specific example, the smart card is a Subscriber Identity Module or SIM of the type used in and for authenticating the use of handsets in a cellular telecommunications network. Such a network will store details of its users' (subscribers') SIMs. In operation of the network, a user's handset is authenticated (for example, when the user activates the handset on the network with a view to making or receiving calls) by sending a challenge to the handset incorporating that SIM, in response to which the SIM calculates a reply (dependent on the predetermined information held on the SIM) and transmits it back to

the network which checks it against its own information for that user or subscriber in order to complete the authentication process. In the same way, therefore, the SIM can be used in or in association with the data processing apparatus or computer so that the same form of authentication process can be carried out. In a case where the SIM is the SIM of a subscriber to a particular cellular telecommunications network, the authentication process can be carried out by that network.

It should be noted that the authentication process being described does not necessarily authenticate the human identity of the user. For example, cellular telecommunication networks have pre-pay subscribers who are issued with SIMs in return for pre-payment enabling them to make calls on the network. However, the identity of such pre-pay subscribers is not known (or not necessarily known) by the networks. Nevertheless, such a user cannot make use of the network until the network has authenticated that user's SIM – that is, has confirmed that that user is a particular user who has a particular pre-paid account with the network. The SIMs of such pre-paid users or subscribers could equally well be used (in the manner described) in or in association with data processing apparatus or computers, for the purposes of authenticating that user.

The SIM need not take the form of a physical (and removable) smart card but instead can be simulated by being embedded in the data processing apparatus or computer in the form of software or represented as a chip for example.

It may be desirable to be able to change the authentication information on the SIM (or simulated SIM) to take account of changed circumstances. For example, the SIM may be a SIM registered with a particular cellular telecommunications network – a network applicable to the country or region where the data processing apparatus or computer is to be used. However, circumstances may arise (for example, the apparatus or the computer is physically moved to a different country or region) in which it is desirable or necessary to re-register the SIM with a different cellular telecommunications network. Ways in which this can be done are disclosed in our co-pending United Kingdom patent applications Nos. 0118406.8, 0122712.3 and 0130790.9 and in our corresponding PCT applications Nos. GB02/003265 and GB02/003260. As described therein in more detail, a SIM (and thus also a simulated SIM) may be initially provided with authentication (and other) information relating to each of a plurality of networks, the information respective to the different networks being selectively activatable.

It is not necessary, however, for the users to be subscribers to a telecommunications network. Instead, they could be subscribers registered with some other centralised system which could then carry out the authentication process in the same way as in a telecommunications network. In such a case, the registration of a SIM (or simulated SIM) could be transferred from one such centralised system to another in the same manner as described above.

As described above, an aim of the authentication process is to facilitate a transaction

between the data processing apparatus or computer and a third party. Where the authentication process is carried out by a telecommunications network, or by some other system, to which the user of the SIM is a subscriber, the satisfactory completion of the authentication process would then be communicated by that network or system to the third party – to enable the transaction to proceed.

For many transactions of the type described, a payment by the user to the third party may be involved. An arrangement as described above, in which the authentication process is carried out by a telecommunications network or other centralised system to which the user is a subscriber advantageously facilitates the making of such payments and is particularly advantageous where (as may often be the case) the payment is for a small amount (for example, payment in return for receipt of information – e.g. weather or traffic information, or for temporary use of specific software); in such a case, the payment can be debited to the account of the subscriber held by the telecommunications network or other centralised system – and then, of course, passed on to the third party, perhaps after deduction of a handling charge.

The block diagram of Figure 1 explains one way of operating the method described above.

A Windows-based personal computer or PC 10 is shown ('Windows' is a trade mark). The PC10 is adapted to receive a SIM shown diagrammatically at 12. The SIM may be

removably fitted to the PC, for use in identifying a user (that is, the holder of the SIM) or may be fixed within the PC (for identifying the PC itself). The PC 10 incorporates transaction management software 14 which interacts with and controls some of the functions of the SIM.

Also shown in Figure 1 is a cellular telephone network 16, such as the Vodafone (trade mark) network, and it is assumed that the SIM 12 is registered with the network 16.

The operation of the system shown in Figure 1 will be explained in relation to the flow chart of Figure 2.

At step A, the user of the PC 10 requests use of a particular application 17 on the PC. For example, the user might wish to view web pages containing specialised information which are encrypted and thus not generally available. In order to do this, the user requests a "session key" – that is, permission to carry out a transaction involving time-limited use of the particular application. The request for the session key is addressed to the transaction manager 14. The transaction manager 14 then, transmits identification information derived from the SIM 12 (an "I am here" message) to the security services part 18 of the network 16 (step B). In response to the "I am here" message, the network transmits a random challenge (step C) to the transaction manager 14, this challenge being based on information known to the network about the SIM 12.

At step D, the transaction manager 14 responds to the challenge by providing an answer derived from the challenge and the key held on the SIM. The reply is checked by the security services part 18 of the network 16. Assuming that the response is satisfactory, the security services part 18 authenticates the user and confirms this to the transaction manager 14 (step E). At the same time, the security services part 18 in the network transmits the session key (step F) to the application services part 22 of the network 16.

The transaction manager 14 also transmits the session key to the application 17 (step G).

The user can now make the request for the particular application (step H), accompanying this application request with the session key received at step G. The application request of step H is transmitted to an application services part 22 which may be part of the network 16 (as shown) or may be separate and controlled by a third party. At step I the application services part compares the session key received with the application request (step H) with the session key received at step F. Assuming that the result of this check is satisfactory, the application services part 22 now transmits acceptance of the application request (step J) to the PC 10, and the application now proceeds (time limited). The network can now debit the user's account with a charge for the session.

The foregoing is of course merely one example of an implementation of what has been described.

In an alternative arrangement, a data carrier may be provided with means for storing predetermined information such as in one of the forms described above – that is, a SIM or (more probably) software simulating a SIM. The simulated SIM is associated with data stored on the data carrier. The data carrier may, for example, be a DVD or CD ROM or some other similar data carrier, and the data thereon may be software or a suite of software.

The simulated SIM may be used to identify and authenticate the data (such as the software) on the data carrier. The simulated SIM will be registered with a telecommunications network or some other centralised system, in the same manner as described above. When the data carrier is placed in data processing apparatus such as a computer, for use therein, the SIM would be used to identify and authenticate the data carrier and the data stored thereon and (for example) could then permit the software to be downloaded for use in the computer. In this way, the SIM could be used subsequently to block further use of the software (for example, in another computer), or to allow the data to be used for only a predetermined number of times (whether in the same or in a different computer). If, for example, the data carrier (with its SIM) is placed in a computer which has also received a particular user's SIM then (a) the SIM on the data carrier can be used to identify and authenticate the software and (b) the SIM in or associated with the computer can be used to authenticate the user and could subsequently be used to enable a charge to be debited to that user as payment for use of the software.

In our co-pending patent application No. GB 0307248.5 we describe an arrangement where, rather than the PC10 being adapted to receive a SIM 12, or a data carrier being modified to incorporate a SIM or software simulating a SIM, a separate device or "dongle" 30 (Figures 3 and 4) is provided for receiving the SIM 12, or for incorporating software simulating the SIM 12.

The dongle 30 allows data for authenticating a transaction (or for any other appropriate purpose) to be passed between the dongle 30 and the PC 10 and onwardly to/from the network 16.

The dongle 30 comprises a plastics housing 32 having a slot for receiving a SIM 12. Appropriate connectors (not shown) are provided within the housing 32 for allowing electronic exchange of data between the SIM 12 and the dongle 30. The dongle 30 further comprises a suitable connector 34 for allowing connection for data communication purposes to the PC 10. For example, the connector could be a USB connector, a Firewire 1394 connector or any other suitable connector. Of course, different configurations of the dongle may be provided. For example, the SIM 12 may be accommodated completely within the dongle 30, and may be removable from the dongle 30 by opening the housing 32, or the SIM 12 may be permanently sealed within the dongle casing 32. If the latter arrangement is provided, a user of the telecommunication system may be provided with a first SIM for use, for example, in their mobile telephone handset and may be provided with a dongle 30 which houses a separate SIM which is used for performing transactions

via a PC 10. If desired, the telecommunications network will include a record indicating that the SIM within the user's mobile handset and the SIM within the user's dongle are commonly owned, and this information may be used to conveniently provide the user with a single account of charges incurred in respect of use of both the SIMs.

The dongle 30 is provided with a dongle interface driver 36 which controls communication with the PC 10. All communications from the PC10 are routed via the dongle interface driver 36 and data stored on the SIM 12 cannot be accessed other than by using the dongle interface driver 36. A corresponding PC interface driver 38 is provided for the PC 10. The PC interface driver 38 may, for example, comprise a series of commands in the form of a computer programme which is loaded onto and run by the PC 10. The PC interface driver 38 may, for example, be provided by or under the control of the network 16. The PC interface driver 38 will therefore be "trusted" by the network 16 and will be configured to only allow access to the dongle 30 and consequently the SIM 12 in an approved manner which will not allow the security information present on the SIM 12 to be compromised.

To prevent, or to reduce, the likelihood of the PC interface driver 38 being replaced or bypassed by an alternative driver, which could compromise the security of the data on the SIM 12, the PC interface driver 38 and the dongle interface driver 36 are provided with respective shared secret keys 40, 42. Each communication from the PC interface driver 38 to the dongle 30 is encrypted using the shared secret key 40. All communications from

the PC 10 to the dongle 30 are received by the dongle interface driver 36. The dongle interface driver 36 comprises processing means for decrypting received communications using its secret key 42. To enhance security, the dongle interface driver 36 will prevent all communications other than those encrypted using the shared secret key 40 from sending data to or receiving data from the SIM 12.

Therefore, the PC interface driver 38 controls and supervises access to the dongle 30 and the SIM 12 to reduce the likelihood of the data stored on the SIM 12 being compromised by unauthorised attempts to access the SIM 12.

Provided that a request for access to data on the SIM 12 is approved by the PC interface driver (according, for example, to criteria set by the network 16), and is therefore communicated to the dongle interface driver 36 with the appropriate key 40, a transaction can be authorised using the SIM 12 in the manner described in relation to Figures 1 and 2.

A further arrangement will be described in relation to Figure 4. According to Figure 4, the dongle 30 has the SIM 12 accommodated completely within its housing 32, and the SIM cannot therefore be seen in the Figure. The dongle 30 has a connector 34 for connection to a PC 10 in a similar manner to the Figure 3 embodiment. At the opposite end of the casing 32 an optional loop connector 44 may be provided to provide a convenient means for carrying the dongle 30 by attaching it to a user's keyring.

One face of the housing 32 has a variety of push buttons 46 mounted thereon, ten of which have respective numerals from 0 to 9 displayed thereon. In this embodiment, the dongle 30 includes means (such as software) for receiving the entry of a PIN number from a user by operating the appropriately designated push buttons 46 which is compared to the PIN number provided for and stored on the SIM 12. The SIMs used in the GSM telecommunications network are conventionally provided with such a PIN.

The housing 32 may further optionally provide a display 48 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered, if desired. On entry of the PIN number using the push buttons 46, the entered PIN number is compared to the PIN number stored on the SIM. If the PINs are found to match, communication between the SIM and the PC10 is permitted to authorise one or more transactions. The comparison between the entered PIN number and the PIN number stored on the SIM 12 is performed within the dongle 30, and neither the entered PIN number nor the PIN number stored on the SIM is communicated to the PC10. This prevents or reduces the likelihood that the PINs will become compromised by disclosure to an authorised party.

The PIN entry comparison arrangement of Figure 4 may be provided in addition to or as an alternative to the interface drivers 36,38 and shared secret keys 40,42 of the arrangement shown in Figure 3.

It should be appreciated that as an alternative to push buttons 46, other means could be provided for allowing PIN entry. Alternatively, the user could be authorised to use the SIM by obtaining some other security information from the user and comparing this with data stored on the SIM 12. For example, the data obtained could be the user's fingerprint or some other characteristic which is unlikely to re-occur on another person. The details of the fingerprint (or other information) are stored on the SIM for comparison with the input data representing the characteristics.

As an additional security feature in the Figure 3 embodiment, a display may be provided which displays the name of the application or organisation which requests information from the SIM 12. This would allow the user to monitor requests being made to their SIM 12.

If the respective interface drivers 36,38 and shared secret keys 40,42 described in relation to Figure 3 are used in a system which also includes the PIN entry and comparison arrangement described in relation to Figure 4, to provide an added level of security, the dongle 30 can be programmed to display the name of the application or organisation requesting data from the SIM 12 and may then prompt the user to approve the supply of data for each or selected applications/organisations by entering the user's PIN using keypad 46.

The dongle 30 may be used to facilitate transactions with data processing apparatus other

than PCs. For example, a user having an account with network 16 and being provided with a dongle 30 can insert the connector 34 into an appropriately configured slot in a parking meter which is connectable to the network 16. The SIM 12 contained within the dongle 30 is authenticated in the manner described above using a transaction manager provided within the parking meter. By this means, payment for parking can be made by deducting an appropriate amount from the user's account with the network 16. Advantageously, the dongle 30 will be provided with push buttons 46 and the dongle will prompt the user to enter a PIN which is compared to the PIN stored on the SIM so that the dongle 30 cannot be used by an unauthorised party. The dongle could be programmed to allow the push buttons 46, under control of the parking meter, to allow entry of data relevant to the transaction – for example, the length of time for which the parking space is required.

The dongle 30 could, for example, also be used in a similar way with an appropriately configured DVD player to allow a film to be viewed on payment of a fee deducted from the user's account with the network 16.

Figures 5A to 5D show a second configuration of a dongle indicated generally at 50. The dongle 50 does not include a display or push buttons. The dongle 50 is of generally elliptical cross-section and includes a generally rectangular aperture 52 formed in the top end thereof that allows an electrical connector 54 of generally rectangular cross-section to emerge therefrom. The aperture 52 is closed by a closure member 56 which is generally

C-shaped in cross-section, extending from the top of dongle 50 along each side face 58, and pivotted about a centrally mounted pivot point 60. The connection between the closure member 56 and the side walls 58 of the dongle 50 at the pivot point 60 allows the closure member 56 to be rotated about the pivot point 60 as shown by arrow 62.

Figure 5C is a cross-section taken along line *X-X* of Figure 5B and shows schematically the mechanism by which the electrical connector 54 can be moved between a first position, shown in Figures 5A and 5B, where the connector 54 is contained wholly within the casing of the dongle 50, and the second position, shown in Figures 5C and 5D, where the electrical connector 54 protrudes from the casing of the dongle 50. The mechanism for providing this movement of the electrical connector 54 comprises a rack 64 which is coupled to the connector 54 and a cooperating pinion 66, mounted at pivot point 60, the teeth of which engage the rack 64. The pinion 66 is fixed with respect to the closure member 56. Rotation of the closure member 56 causes rotation of the pinion 66, which causes linear displacement of the rack 64 as shown by arrow 68. Of course, a mechanism for slidably supporting the electrical connector 54 and rack 64 is provided in a manner that will be understood by those skilled in the art, and is not illustrated or described further here.

Figures 6A to 6D show a third configuration of a dongle. As in the second configuration of dongle described in relation to Figures 5A to 5D, the electrical connector 54 is movable between a first position, shown in Figures 6A and 6B, where it is contained completely

within the casing of the dongle 70, and a second position, shown in Figures 6C and 6D, where the connector 54 is shown extending from the casing of dongle 70. However, in the third configuration, the linear movement of the electrical connector 54 in the direction of arrow 68 is provided by rotating knob 72 with respect to the casing of dongle 70 as shown by arrow 74. Rotation of the knob 72 in a first direction causes the connector 54 to emerge from the casing of dongle 70, and rotation in the opposite direction causes the connector 54 to be retracted within the casing of the dongle 70. Any suitable mechanism for converting the rotary motion of the knob 72 into linear motion of the connector 54 may be provided. For example, a mechanism described in U.S. Patent No. 5813421 (which is incorporated herein by reference) for a lipstick swivel mechanism may be employed. Other suitable mechanisms will be known to those skilled in the relevant art.

The dongle 70 includes a display 48 for prompting the user to enter their PIN number and/or for displaying the PIN number as it is entered. The dongle 70, rather than having a series of push buttons (such as a numerical key pad) comprises a data entry knob 76 which is mounted to the dongle for rotation as shown by arrow 78 and also for linear motion with respect to the dongle as shown by arrow 80. Each digit of the PIN number is input by the user grasping the knob 76 and pulling it in a direction away from the casing of the dongle 70 (in the direction of arrow 80). An indication, such as a flashing cursor then appears on the display 48 indicating that the first digit of the PIN number is expected. The number is input by rotation of the knob 76 (arrow 78), the displayed number increasing in value with further rotation of the knob 76. When the required

number appears on the display 48 the user confirms that this is the number they wish to input by pushing the knob 76 in the opposite direction to arrow 80. To input the next digit of the PIN number the knob 76 is again lifted (arrow 80) and the correct number is selected by rotation of the knob. The required number is entered by returning the knob 76 to its original position by moving it in the direction opposite to the arrow 80. This procedure is repeated until all of the digits of the PIN number have been entered. Each digit of the PIN number as it is entered will be displayed on the display 48.

In the Figure 6A to 6D embodiment of the dongle 70, a piezo electric cell 82 is associated with the knob 80. The piezo electric cell 82 allows power to be generated by movement of the knob 76. This power may either be stored in an integral capacitor or may be stored in an optional cell 84 which is electrically coupled to the piezo electric cell 82. Such an arrangement obviates the requirement for the dongle 70 to have its own replaceable power source, whilst allowing the dongle to be operated when not connected to the PC 10. The charge generated by the piezo electric cell is transient, and after a period of time (for example, 5 minutes), the charge is dissipated and any PIN number entered by means of the knob 76 is lost from the memory of the dongle 70 and cannot later be retrieved even when power is supplied. This provides an additional security feature to the dongle 70. Of course, if the dongle 70 is connected to the PC10 while the charge is still present (within 5 minutes of entering the PIN in the example given above), the PIN can be verified and the dongle can then obtain power from the PC10 via the connector 54 which allows authentication operations described above to be performed despite the transient nature of

the power from the piezo electric cell 82.

Figures 7A to 7D show a fourth configuration of dongle 90. In this embodiment the dongle 90 comprises a main body part 92 to which the electrical connector 54 is attached in a fixed position, and a removable protective cap 94 which, when in position, covers the main body 92 and the connector 54 to protect those components and to provide the dongle 90 with an attractive external appearance.

At the top end of the main body 92 an annular knob 96 is mounted to the body 92 for rotation with respect to the body 92, as shown by arrow 98. The knob 96 includes a series of markings 100 visible to the user of the dongle 90 - for example, each mark 100 indicating a different digit from 0 to 9. A marking 102 is provided at the top of the casing 92. In this embodiment, the first digit of the user's PIN number is entered by rotating the knob 96 until the correct digit of the PIN number (indicated at 100) is aligned with the mark 102. When the relevant digit and the mark 102 are aligned, the user stops rotation of the knob 96. When movement of the knob 96 stops, the position of the knob 96 is recorded by the dongle 90 so that the digit of the PIN number can be detected. The next digit of the PIN number is entered by rotating the knob 96 in an anti-clockwise direction (opposite to arrow 98) until the relevant digit of the PIN number is aligned with marking 102. Again, when the rotation of the knob stops, the position of the knob is recorded so that the PIN number can be recorded by the dongle 90. The next digit of the PIN number is entered by clockwise rotation of the knob 96, and so on, until all of the digits of the PIN

number is entered by clockwise rotation of the knob 96, and so on, until all of the digits of the PIN number have been entered. The manner of data entry using the knob 96 and the marking 102 is similar to that used to enter the combination of a safe.

The dongle 90 further includes an optional digital camera 104 mounted at the axis of rotation of the knob 96 (but fixed with respect to the main body 92). Dongle 90 includes processing means and memory for storing one or more images captured by the camera 104, and allows these images to be transferred to the PC 10 using the connector 54.

Figures 8A to 8C show a fifth configuration of a dongle 110. The dongle 110 comprises a casing 112 which has an opening 114 at one side thereof. Contained within the casing 112 is a coupling portion 116 to which the electrical connector 54 is fixed. The coupling portion 116 is connected to the casing 112 in such a manner that the coupling portion 116 is rotatable about an axis indicated by dotted line 118.

Connected to the loop connector 44 is a ring 120, which provides a convenient means by means a slidable part 122, which is mounted for sliding with respect to the casing 112, may be moved with respect to the casing 112 in the direction of arrow 124. By means of a rack and pinion or any other suitable mechanism (not shown) the movement of the sliding part 122 with respect to the casing 112 in the direction of arrow 124 is translated into rotational movement of the coupling portion 116 about the axis 118. The different positions that the coupling part 116 moves through as the sliding part 122 is moved with

respect to the casing 112 are shown by the ghost lines in Figure 8C.

When the sliding part 122 reaches its maximum travel in the direction of arrow 124, the coupling part 116 is rotated 180° with respect to the casing 112. The coupling portion 116 is returned to the position shown in Figures 8A and 8B by sliding the sliding part 122 in the direction opposite to arrow 124. When the coupling part 116 is in the position shown in Figures 8A and 8B, the connector 54 is protected by the sliding part 122.

The embodiments shown in Figures 5,6,7 and 8 provide various means by which the electrical connector 54 can be concealed and protected when not required.

In the Figure 6 embodiment the power source of the dongle is piezo electric cell 82.

A similar power source may be provided in the dongles illustrated in Figures 5,7 and 8, with power being generated by movement of the closure member 56 of the dongle 50 of Figure 5, the movement of the knob 96 of the dongle 90 of Figure 7, or movement of the sliding part 122 of Figure 8. Alternatively, or additionally, these dongles may include a replaceable battery or a rechargeable battery which is recharged when the dongle 50,80,90,110 is connected to the PC10.

Whilst the dongles described include an electrical connector 54 which is shown as a USB connector, it should be appreciated that any other suitable type of electrical connector

may be provided. For example, the connector 54 may be a SmartMedia (trade mark) device. Alternatively, data and/or power may be transmitted between the dongle and the PC 10 by "near field" technology, for example, in accordance with the Near Field Communication Interface and Protocol (NFCIP-1) protocol. If near field technology is employed, the provision of a movable electrical connector 54 will not be necessary.

The dongles of Figures 5 to 8 may or may not include the dongle interface driver 36 described in relation to Figures 3 and 4.

The dongles of Figures 6 and 7 may allow the PIN to be passed to the PC10 for validation, or such validation may be performed within the dongle for improved security.

Of course, the dongles of Figures 5 and 8 may be provided with a PIN entry means if required.

## CLAIMS

1. A device for connection to a data processing apparatus, the device including first coupling means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus; second coupling means for operative coupling to the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined information; security data entry means for obtaining security data independently of the data processing apparatus; and means for storing the security data temporarily.

2. The device of claim 1, wherein the security data is stored temporarily by means of a transient power source.

3. The device of claim 2, wherein the transient power source comprises piezo electric means.

4. The device of claim 3, wherein the piezo electric means comprises one or more piezo electric cells.

5. The device of claim 2,3 or 4, wherein the transient power source is charged by the security data entry means.

6. The device of claim 2,3,4 or 5, wherein the transient power source comprises a rechargeable battery.

7. The device of any one of claims 1 to 6, comprising means for analysing the entered security data for determining whether to allow access to the predetermined information.

8. A device for connection to a data processing apparatus, the device including first coupling means for operative coupling to authentication storage means storing predetermined information relating to the authentication of a transaction with the data processing apparatus; second coupling means for operative coupling to the data processing apparatus; and configuration means for selectively rendering the second coupling means available for coupling to the data processing apparatus, the device when operatively coupled to the data processing apparatus being responsive to an authentication process carried out via a communications link for authenticating the transaction, the authentication process involving the use of the predetermined configuration information.

9. The device of claim 8, wherein the configuration means comprises means for selectively making the second coupling means available externally of the device housing.

10. The device of claim 9, wherein the configuration means comprises a removable cap.

11. The device of claim 9, wherein the configuration means comprises a closure member coupled to and moveable with respect to the housing for selectively closing an aperture in the housing.

12. The device of claim 11, comprising interconnection means for connecting the closure member and the second coupling means, the arrangement being such that, as the closure member is moved to open the aperture, the second coupling means emerges from the aperture.

13. The device of claim 8, comprising a knob mounted on the device housing for rotation with respect thereto, and means for converting rotation of said knob into linear movement of the second coupling means such that rotation of said knob in a first direction causes the second coupling means to emerge from an aperture in the device housing and rotation of said knob in a second direction causes the second coupling means to be retracted through said aperture.

14. The device of claim 9, wherein the device housing includes two parts moveable with respect to one another between a first arrangement where the second coupling means

is contained within the housing and a second arrangement where the second coupling means is exposed for connection to the data processing apparatus.

15. The device of claim 14, wherein the two parts are pivotally coupled together.

16. The device of any one of claims 8 to 15, comprising security data entry means for obtaining security data independently of the data processing apparatus, and means for analysing the entered security data for determining whether to allow access to the predetermined information.

17. The device of any one of claims 8 to 15, comprising security data entry means for obtaining security data independently of the data processing apparatus; and means for storing the security data temporarily.

18. The device of any one of claims 1 to 17, wherein the device controls access to the predetermined information.

19. The device of any one of claims 1 to 7 and 16 to 18, wherein the security data entry means comprises alphanumeric data entry means.

20. The device of any one of claims 1 to 7 and 16 to 19, wherein the security data entry means comprises a keypad.

21. The device of any one of claims 1 to 7 and 16 to 20, wherein the security data comprise a Personal Identification Number (PIN) and analysing means compares the PIN obtained by the security data means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

22. The device of any one of the preceding claims, comprising a display for displaying security information.

23. The device of any one of the preceding claims, comprising a data processing module for controlling the communication with the data processing apparatus.

24. The device of claim 23, wherein the data processing module of the device is configured for communicating with a corresponding data processing module of the data processing apparatus.

25. The device of claim 24, wherein communication between the authentication storage means and the data processing apparatus is performed via the respective data processing modules.

26. The device of claim 23,24 or 25, wherein the data processing module of the device includes means for decrypting encrypted data received from the data processing module

of the data processing apparatus.

27. The device of claim 23,24,25 or 26, wherein the data processing module of the device includes means for encrypting data transmitted to the data processing module of the data processing apparatus.

28. The device of claims 26 or 27, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

29. The device of claim 28, wherein the key comprises a shared secret key for each of the respective data processing modules.

30. The device of any one of the preceding claims, wherein the device is operatively coupleable to one of more of a plurality of said authentication storage means, each of which is registerable with a common telecommunication system, and wherein the authentication process is performed by a communications link with the telecommunications system.

31. The device of claim 30, in which the predetermined authentication information stored by each authentication storage means corresponds to information which is used to authenticate a user of that authentication storage means in relation to the telecommunications system.

32. The device of claim 31, in which each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

33. The device of any one of claims 1 to 32, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

34. The device of any one of claims 1 to 33, in which the authentication storage means is specific to that device.

35. The device of any one of claims 1 to 34, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

36. The device of any one of claims 30 to 35, wherein the telecommunications system includes means for levying a charge for the transaction when authorised.

37. The device for any one of claims 1 to 7, 16 and 17, wherein the security data entry means comprises a rotary knob.

38. The device of any one of the preceding claims in combination with the data processing apparatus.

39. The device of any one of the preceding claims in combination with the telecommunications system.

40. A device substantially as described with reference to the accompanying diagrammatic drawings.

The Patent Office

INVESTOR IN PEOPLE

| | | | |
|---|---|---|---|
| **Application No:** | GB 0311729.8 | **Examiner:** | Henrik Ebbesen Jensen |
| **Claims searched:** | 1-40 | **Date of search:** | 1 September 2003 |

# Patents Act 1977 : Search Report under Section 17

**Documents considered to be relevant:**

| Category | Relevant to claims | Identity of document and passage or figure of particular relevance | |
|---|---|---|---|
| X, A | X: 1<br>A:8 | US 6226744 B | (MURPHY) See abstract, fig. 3, col 3, l 6-29, col 6, l 22-32 |
| A | | WO 00/002407 A | (NOKIA) See fig. 1, 2 and p 3, l 30 - p 5, l 35. |
| P, A | | WO 02/091316 A | (ACTIVCARD) See fig. 1, 2, 4a-5, p 3, l 1-19, p 6, l 30 - p 7, l 36, p 9, l 11 - p 11, l 10 and p 12, l 1 - p 15, l 32. |
| A | | WO 00/070533 A | (SCHLUMBERGER) See abstract. |
| A | | WO 01/080525 A | (SUN) See abstract, p 7, l 12-21 and claim 1-10. |

Categories:

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category | P | Document published on or after the declared priority date but before the filing date of this invention |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application |

**Field of Search:**

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[V]:

Worldwide search of patent documents classified in the following areas of the IPC[7]:

G06F, G07F, H04L

The following online and other databases have been used in the preparation of this search report:

WPI, EPODOC